# 16. PRIVACY and SECURITY OF CLIENT INFORMATION

* 1. POLICY TITLE: Privacy and Security of Client Information
		1. Officially Adopted: March 1, 2018
		2. Effective Date: April 1, 2018
		3. Signed:

##  Kelli Nomura, Behavioral Health Organization Administrator

* 1. PURPOSE: To describe the requirements for safeguarding information systems, data security, and the protection of client records and confidentiality.
	2. POLICY/PROCEDURE/RESPONSIBILITIES:
		1. Information Security and Privacy Policies
			1. Providers shall develop comprehensive information security and privacy policies and procedures to ensure data security and the protection and confidentiality of client records. The policies and procedures shall address Health Insurance Portability and Accountability Act (HIPAA) privacy and security requirements and shall be updated as necessary.
			2. The King County Behavioral Health and Recovery Division (BHRD) shall designate a Privacy Officer who, together with the King County Information Technology (KCIT) Security Team, is responsible for ensuring that privacy and security policies and procedures are adequate and are implemented within BHRD.
			3. Providers shall designate a provider Privacy and Security Officers to be responsible for ensuring that privacy and security policies and procedures are adequate and are implemented within the provider agency.
		2. Access to the Behavioral Health and Recovery Division (BHRD) Information System (IS)
			1. Authorized users may be given access to the BHRD applications listed on the BHRD IS Electronic Access Request (EAR) Application and User Agreement form (Attachment A, Appendix 17A).
			2. Access to BHRD IS is restricted by the following:
				1. The person accessing the information must have professional qualifications related to the information he/she is seeking; and
				2. The person accessing the information must have a ‘need to know’ the specific information for the assessment or treatment task that is his/her responsibility:

To link designated personnel to the behavioral health care provider responsible for providing services to a BHRD client;

To provide service history information on a client currently requesting or receiving services from a BHRD provider;

To determine the medically necessary level of service for a client; or

To audit and validate submissions, if this task is within the scope of the user’s job function.

* + - 1. Access to information may be given in some instances primarily for research and or evaluation activities, as specified in Attachment B, Evaluation and Research Committee policy and procedure.
			2. BHRD IS Initial Application Process

Authorized staff may request access to the BHRD IS by completing an EAR form (Attachment A, Appendix 17A) following these procedures:

* + - * 1. Applicant completes the form, reads and acknowledges the conditions for access by initialing the section, signs and dates the form;
				2. Supervisor reviews applicant information, signs and dates the form, then submits the completed document to BHRD;
				3. BHRD Privacy Officer approves application and submits work ticket to the KCIT Service Center;
				4. KCIT Service Center creates a user account with appropriate security permissions;
				5. BHRD notifies applicant of approval, user name, and instructions to complete activation of account.
				6. Authorized staff are granted an account and held personally responsible for all activity on that account, including civil and criminal liability.
			1. BHRD IS Renewals and Cancellations
				1. Renewals

User accounts must be renewed on an annual basis. Renewal requires submission of a signed EAR form (Attachment A, Appendix 17A) from the named user.

Application is sent to BHRD for processing. The user account is renewed with appropriate security permissions.

* + - * 1. Cancellations

Any account that does not show connect-activity for a period of more than 60 days will be disabled. The user can contact KCIT Service Center to request reactivation of the account.

If at any time BHRD has any reason to believe an account is being used by a person other than the authorized user, the account shall be immediately disabled. Where an account has been canceled for cause, a signed EAR form must be submitted for reinstatement.

When an authorized user leaves employment, the provider is required to notify BHRD IS in writing at least five business days in advance of the date of termination. KCIT Service Center will cancel the user’s accounts in all information systems, effective the date of termination.

* + - 1. Passwords for BHRD IS

Passwords are mandatory for accessing data BHRD IS server.

* + - * 1. Passwords shall never be disclosed to others and shall be changed at least every 90 days. Passwords are set to expire at 90 days if not changed. Once the password has expired, the user will not be able to log into the BHRD system and must contact KCIT Service Center to request reactivation of the account.
				2. Providers shall configure software so that the entry of passwords on the input screen shall be invisible or encrypted, and password files shall be encrypted where possible.
				3. Employees shall be held accountable for access to BHRD applications gained through the use of their user ID and password combination.
		1. Data Extracts

Provider staff may request data extracts containing confidential data by following these procedures:

* + - 1. Submit an Evaluation and Research Proposal Application and all required materials specified in Attachment B: Evaluation and Research Committee.
			2. Prior to submitting a proposal, the requester must have a consultation with an Evaluation and Research Committee member. If identified or identifiable data is being requested from BHRD, the requester must also have a consultation with the BHRD Privacy Officer prior to proposal submission.
			3. The project requiring the use of the data extract must be approved by the Evaluation and Research Committee.
		1. Release of Client Information from BHRD IS
			1. Confidential client information cannot be released without the signed consent or authorization of the client or legally responsible other person except under conditions allowed by state or federal law. Consent or authorization must meet the criteria described in Attachment A: Protection of Confidential Client Information, item 4.3 Consent.
			2. Authorized users who receive requests for confidential information shall ensure that all criteria for release of information stated in this manual are met before releasing any information.

Using established data security protocols:

* + - * 1. Determine the identity and role of the inquirer;
				2. Determine if linkage to a service provider is appropriate;
				3. Determine if the inquirer has a right to know the information and/or if confidential information must be released in order to provide appropriate services to the client in question;
				4. Link the inquirer to a service provider, if appropriate;
				5. Disclose to the inquirer only that information deemed necessary to provide service to the client; and/or
				6. Refer inquirer to an appropriate agency for assistance if all Release of Information criteria are not met and explain why the request for information is denied.
			1. Providers shall provide assistance to law enforcement and corrections personnel in the most expedient manner possible, but only as allowed by Revised Code of Washington (RCW) 70.02 and or any successors.
			2. Request for release of information to state corrections personnel are found in Washington Administrative Code (WAC) 388-865-0600 to 0640 or any successors.
			3. Disclosure of confidential information must be recorded according to procedures described in Attachment A, Appendix 10.
		1. Client Records
			1. Confidential client records may be required and requested by BHRD in the course of reviews conducted for outpatient benefit authorization, inpatient certification and authorization for requests for extension, and clinical and administrative site reviews for inpatient and outpatient treatment.
			2. A signed consent or authorization by the client is not required for the disclosure of information to BHRD when disclosure purposes directly relate to State plan administrative responsibilities contracted to BHRD.
			3. Compliance with specific requirements for substance use disorder (SUD) treatment, as specified in 42 Code of Federal Regulations (CFR) Section 2 or its successor must be ensured.
			4. BHRD will request records from a provider as follows:
				1. BHRD will telephone the client’s care provider who will be expected to facilitate the request through the provider’s medical records department.
				2. BHRD will be responsible for verbally defining the purpose of the request and limiting the chart information needed so as to minimize copying work and expense.
				3. Records shall be forwarded to BHRD within five working days. As per Chapter 70.02 RCW or its successor, a reasonable fee may be charged for these records.
				4. When the chart information requested is considerable (as mutually determined), attempts will be made to arrange a site visit by BHRD. Such a visit will include the on-site clinical team for clinical consultation and/or disposition planning.
			5. Client records obtained by BHRD will be maintained in a clinical file under the client’s name. These files will be kept in a secure location at BHRD office.
			6. Records obtained by BHRD for the purpose of clinical review will not be available for review by Ombuds services or the Quality Review Team (QRT).
		2. Electronic Message Systems
			1. Protected Health Information (PHI) may be sent in the body of an email or in an attachment if encrypted.
			2. No PHI may be included in texting or instant messaging.
		3. Internet Access

Providers shall not access the internet through KCIT except to access web-based applications enabled through the King County Intranet Home Page.

* + 1. Computer Viruses

Providers shall develop procedures for protecting client records and BHRD data from alteration or destruction by computer virus infections.

* + 1. Data Sharing Agreements

BHRD may at times enter into data sharing agreements with other agencies. All authorized users of the BHRD IS are bound by these data-sharing agreements and may not, in any way, deviate from stipulations. Data sharing agreements help protect the BHRD IS from potential criminal and civil liability should the data be compromised by another agency. Any user who violates these agreements may be subject to criminal and civil liability.

* + - 1. BHRD negotiates data sharing agreements with other entities to:
				1. Specifically state, in writing the requirements associated with the sharing of data; and/or
				2. Record which external agencies are accessing BHRD.
			2. A list of existing data-sharing agreements is available upon request from BHRD Fiscal staff.
	1. LIST OF ATTACHMENTS:
		1. Attachment A: Protection of Confidential Client Information
			1. Appendix 1: Designated Record Set
			2. Appendix 2: Limited Data Set from 45 CFR Part 164.514(e) HIPAA
			3. Appendix 3: BHRD Authorization for Use and Disclosure of Protected Health Information
			4. Appendix 3A: BHRD Authorization for Use and Disclosure of Protected Health Information (Multiple Parties)
			5. Appendix 3B: BHRD Releases of Information Description
			6. Appendix 3C: Authorization for Use and Disclosure of Substance Use Disorder Protected Health Information
			7. Appendix 3D: Consent for Substance Use Disorder Client Lookup
			8. Appendix 3E: Authorization to Disclose and Redisclose Substance Use Disorder Protected Health Information
			9. Appendix 4: Maximum Potential Access to and Use of Protected Health Information by BHRD Staff without Client Authorization or Consent
			10. Appendix 5: Routine Disclosure of Protected Health Information by BHRD Staff
			11. Appendix 6: Redisclosure of Information for Clients Enrolled in Substance Use Disorder and/or Mental Health Services
			12. Appendix 6A: King County Provider Network and State-Contracted Managed Care Organizations
			13. Appendix 7: Request for Client Information without Authorization
			14. Appendix 8: Form for Invalid Authorizations
			15. Appendix 9: Request to Communicate by Alternate Means or at an Alternate Location
			16. Appendix 10: Log of Disclosures without Client Consent or Authorization
			17. Appendix 11: Request to Revoke Consents (or Authorizations) for the Release of Information
			18. Appendix 12: Request to Amend or Correct Protected Health Information
			19. Appendix 13: Request to Restrict Access, Use, or Disclosure of Protected Health Information
			20. Appendix 14: Request for Accounting of Disclosures
			21. Appendix 15: Oath of Confidentiality
			22. Appendix 16: Disclosure of Minimum Necessary Electronic Protected Health Information Without Client Authorization or Consent
			23. Appendix 17A: Information Systems Electronic Access Request (EAR) Application and User Agreement (Providers)
			24. Appendix 17B: Information Systems Electronic Access Request (EAR) Application and User Agreement (BHRD)
			25. Appendix 18: BHRD Procedure for Making a CD containing PHI
			26. Appendix 19: DSHS Intranet Oath of Confidentiality
			27. Appendix 20: Business Associate Agreement
			28. Appendix 21: Research and Evaluation Data Sharing Agreement
			29. Appendix 21A: Data Security Requirements
			30. Appendix 21B: Certification of Data Disposition
			31. Appendix 21C: Research and Evaluation Oath of Confidentiality
			32. Appendix 22: Data Use Agreement for Limited Data Set
			33. Appendix 23: DSHS PRISM Registration Form
		2. Attachment B: Evaluation and Research Review Committee
	2. REFERENCES:

Washington State Law, Regulations, and Policy including any successor, amended, or replacement laws, regulations, or policies

* Chapters 388-865 WAC – Department of Social and Health Services (DSHS) – Mental Health – Community Mental Health and Involuntary Treatment Programs
* Chapter 388-877 WAC DSHS – Behavioral Health Services
* Chapter 388-877A WAC DSHS – Behavioral Health Services – Outpatient Mental Health Services
* Chapter 388-877B WAC DSHS – Behavioral Health Services – Chemical Dependency Services
* Chapter 10.77 RCW – Criminal Procedure – Criminally Insane
* Chapter 13.50 RCW – Juvenile Courts and Juvenile Offenders – Keeping and Release of Records by Juvenile Justice or Care
* Chapter 70.02 RCW – Public Health and Safety – Medical Records – Health Care Information Access and Disclosure
* Chapter 71.05 RCW – Mental Illness – Mental Illness
* Chapter 71.24 RCW – Mental Illness – Community Mental Health Services Act
* Chapter 71.34 RCW – Mental Illness – Mental Health Services for Minors
* Chapter 70.96A RCW – Public Health and Safety – Treatment for Alcoholism, Intoxication and Drug Addiction

Federal Regulations including any successor, amended, or replacement laws, regulations, or policies

* CFR Title 45 Part 160, Part 162 and Part 164 – HIPAA Administrative Simplification Regulations
* CFR Title 42 Part 438 Managed Care
* CFR Title 42 Part 2 Confidentiality of Substance Abuse Records